Adobe Acrobat DC und Sicherheit

Die führende PDF-Lösung zum Erstellen, Bearbeiten und Verwalten von Dokumenten

Inhalt

Sicherheit ist ein zentrales Thema, vor allem wenn Sie einer anderen Partei sensible Informationen anvertrauen. Adobe widmet sich seit mehr als 20 Jahren dem Thema digitale Dokumente und hatte eine Vorreiterrolle bei Standards für PDF und digitale Signaturen. Unzählige Organisationen weltweit haben bereits Milliarden von PDFs erstellt, weil sie auf Adobe Acrobat und Adobe PDF vertrauen, um wichtige Geschäftsdokumente effektiv vorzubereiten, zu schützen und weiterzugeben.

Adobe Acrobat DC und Adobe Document Cloud bieten die PDF-Komplettlösung für die mobile und vernetzte Arbeitswelt von heute. Sie vereint Acrobat DC für den Desktop mit Zugriff auf zusätzliche Funktionen der Adobe Acrobat Reader-App mit Diensten von Adobe Document Cloud. Somit erfüllt die Lösung jeden Anspruch an einen mobilen, intelligenten Dokumenten-Workflow mit geräteübergreifendem Schutz für wichtige Daten. Mit Acrobat DC sind Sie immer auf dem neuesten Stand, denn Sie erhalten Zugriff auf alle aktuellen Sicherheits-Updates und Funktionen, die Sie nach Ihrem eigenen Zeitplan installieren können.

Dieses Dokument behandelt die mehrschichtige Sicherheitsstrategie von Adobe, die wichtige Daten auf Dokument-, Applikations- und Cloud-Ebene effektiv schützen und für ein sichereres Anwendererlebnis sorgen.

Dokumentensicherheit

Bei der Erstellung eines PDF-Dokuments mit Acrobat DC stehen vielfältige Sicherheitsfunktionen zur Auswahl, z. B. Verschlüsselung, Zugriffskontrollen, Zertifikatssignaturen oder Werkzeuge zum Schwärzen von Text und Bildern. Dass die Definition von Aktionen, die mehrere sicherheitsrelevante Aufgaben umfassen, in Acrobat DC so einfach ist, trägt dazu bei, dass vertrauliche Informationen nicht ungeschützt weitergegeben werden. Mithilfe dieser Aktionen können Mitarbeiter standardkonforme PDF-Dokumente erstellen, ohne eine spezielle Schulung erhalten oder über Spezialwerkzeuge verfügen zu müssen.

Verschlüsselung

Acrobat DC unterstützt:

- 256-Bit AES (Advanced Encryption Standard)
- ETSI-Standards (European Telecommunications Standards Institute)

Zugriffskontrollen

Kennwörter verhindern den Zugriff auf ein PDF-Dokument durch nicht autorisierte Anwender. Anhand von Nutzungsrechten legen Sie fest, ob man das Dokument drucken, kopieren und/oder bearbeiten darf.

Elektronische Unterschriften und digitale Signaturen

In Acrobat DC stehen Anwendern zwei verschiedene Werkzeuge für die sichere Arbeit mit Unterschriften zur Verfügung: „Zum Unterschreiben senden“ und „Zertifikate“.

Das Werkzeug „Zum Unterschreiben senden“ ermöglicht eine lückenlose Verwaltung von elektronischen Unterschriftsprozessen, die Gesetzen und Bestimmungen zu *elektronischen Unterschriften* in den USA, der Europäischen Union und den meisten anderen Industrieländern entsprechen. Anwender können Unterschriften einholen, Unterschriftsprozesse nachverfolgen sowie unterzeichnete Dokumente und Prüfprotokolle automatisch archivieren. Der gesamte Prozess lässt sich sicher und zuverlässig verwalten. Zusätzlich werden Dokumente und Prüfprotokolle mit einem Siegel vor Manipulation geschützt. „Zum Unterschreiben senden“ wird unter Verwendung von *Adobe Sign* durchgeführt, einer *Adobe Document Cloud*-Lösung, die durch unabhängige Stellen zertifiziert wurde und strengen Sicherheitsvorschriften entspricht, darunter ISO 27001, SOC 2 Typ 2 und HIPAA sowie PCI DSS.

Das Werkzeug „Zertifikate" ermöglicht das Unterzeichnen mit zertifikatbasierten digitalen IDs von Anbietern auf Vertrauenslisten wie der Adobe Approved Trust List (AATL) und den European Union Trusted Lists (EUTL). Das Unterzeichnen mit einer zertifikatbasierten ID, die von einer Zertifizierungsstelle vergeben wurde, gehört zu den sichersten Methoden der elektronischen Unterzeichnung von Dokumenten. Die ID wird dem Unterzeichner eindeutig zugeordnet und kann seine Identität bestätigen. Im Unterzeichnungsprozess wird das Zertifikat des Unterzeichners mithilfe des nur ihm zugewiesenen privaten Schlüssels an das Dokument gebunden. Acrobat DC stellt automatisch eine Verbindung zu einer Zertifizierungsstelle her, um die Signatur und die Authentizität des unterzeichneten Dokuments zu prüfen. Diese Form der Signatur erfüllt die Standards für elektronische Unterschriften in PDFs, darunter PAdES (PDF Advanced Electronic Signature), Teil 2, 3 und 4, und die JITC*-konforme Verschlüsselung und Verwendung einer PKI mit AES-256, RSA-4096 oder SHA-512. Zudem können Anwender mit dem Werkzeug „Zertifikate" Dokumenten Zeitstempel hinzufügen und sie mit einem manipulationssicheren Siegel versehen.

Weitere Informationen zu diesem Thema finden Sie im Whitepaper *Vollständig digitale Geschäftsprozesse mit Adobe-Lösungen für elektronische und digitale Signaturen*.

Schwärzung

Mit den Schwärzungswerkzeugen von Acrobat DC lassen sich vertrauliche Informationen zuverlässig schützen. Sowohl Text als auch Bilder können vor der Weitergabe eines Dokuments unwiderruflich gelöscht werden. Sie können auch Informationen suchen und entfernen, die bestimmten Mustern entsprechen, wie z. B. Telefonnummern, Kreditkartennummern und E-Mail-Adressen. Während andere Tools und Methoden der Schwärzung Inhalte lediglich verdecken, werden bei Acrobat DC die ausgewählten Informationen vollständig aus der Datei entfernt.

Mit der Funktion „Dokument bereinigen" lassen sich auch verborgene Informationen wie Metadaten aus einem PDF entfernen.

Anwendungssicherheit

Die verbesserten Sicherheitsfunktionen von Acrobat DC bieten Schutz vor Versuchen, über PDF-Dateien Malware auf Ihrem System zu installieren und/oder auf vertrauliche Daten zuzugreifen.

Bei Adobe sind Sicherheitsmaßnahmen ein fester Bestandteil der Unternehmenskultur, Software-Entwicklung und Produktkonzeption. Acrobat DC und Acrobat Reader nutzen führende Sicherheitstechnologien zur Authentifizierung sowie zur Wahrung der Vertraulichkeit von Daten und Integrität von Dokumenten.

Produktsicherheit

Bei der Entwicklung aller Produkte von Adobe Document Cloud wird der SPLC-Prozess (Adobe Secure Product Lifecycle) angewandt, ein Regelwerk aus mehreren Hundert strengen, auf größtmögliche Sicherheit ausgerichteten Methoden, Prozessen und Werkzeugen. Sie kommen während des gesamten Acrobat DC-Produktzyklus zum Einsatz – von Design und Entwicklung bis hin zu Qualitätssicherung, Test und Bereitstellung. Weitere Informationen zu den Sicherheitsprozessen und dem Engagement von Adobe innerhalb der Community für IT-Sicherheit sowie dem Adobe Secure Product Lifecycle (SPLC) finden Sie unter *www.adobe.com/de/security/*.

Geschützter Modus in Adobe Acrobat Reader DC

Was ist „Sandboxing"?

„Sandboxing" wird von Sicherheitsfachleuten hoch geschätzt. Es handelt sich um eine Methode, eine abgegrenzte Umgebung mit eingeschränkten Rechten für die Ausführung von Programmen zu schaffen. Die Sandbox trägt zum Schutz des Endanwender-Systems vor Angriffen mit nicht vertrauenswürdigen Dokumenten bei, die möglicherweise ausführbaren Code enthalten. Im Kontext von Acrobat Reader DC gelten alle PDF-Dateien und die Prozesse, die sie aufrufen, als nicht vertrauenswürdige Inhalte. Acrobat Reader DC behandelt alle PDF-Dokumente als potenziell schädlich und beschränkt alle Prozesse, die die PDF-Datei aufruft, auf die Sandbox.

Um Sie und Ihre Organisation vor Schad-Software zu schützen, die versucht, mithilfe von PDF-Dateien das Dateisystem Ihres Computers zu manipulieren, bietet Adobe seit Adobe Reader X den geschützten Modus, eine Implementierung der fortschrittlichen Sandbox-Technologie.

In Acrobat Reader DC erweitert dieser Modus den Schutz vor Angreifern, die versuchen, Schad-Software auf dem Anwendersystem zu installieren. Damit werden das Lesen und der Abruf vertraulicher Daten und geistigen Eigentums auf Ihrem Computer oder im Firmennetzwerk verhindert.

Der geschützte Modus wird standardmäßig beim Starten von Acrobat Reader DC aktiviert. Insbesondere schränkt dieser Modus die Zugriffsrechte für das Programm ein, sodass Microsoft Windows®-Systeme vor böswilligen PDF-Dateien geschützt werden, die gegebenenfalls versuchen, in das Dateisystem des Computers zu schreiben oder Informationen auszulesen, Dateien zu löschen oder auf andere Weise Systemdaten zu verändern. Der geschützte Modus von Acrobat Reader kann jetzt unter Windows 8.1 und höher in einem AppContainer ausgeführt werden. Weitere Informationen zum Thema AppContainer finden Sie unter *https://msdn.microsoft.com/en-us/library/windows/desktop/mt595898(v=vs.85).aspx*.

Darüber hinaus führt Adobe im Rahmen seiner Bemühungen, mithilfe des Adobe Secure Product Lifecycle (SPLC) Sicherheit auf mehreren Stufen der Produktlebensdauer zu integrieren, regelmäßig Prüfungen des bestehenden Codes durch und schottet ihn gegebenenfalls ab, um die Anwendungssicherheit noch weiter zu verbessern und die Sicherheit Ihrer Daten zu erhöhen, wenn Sie mit Adobe-Produkten arbeiten.

*Joint Interoperability Test Command des US-Verteidigungsministeriums

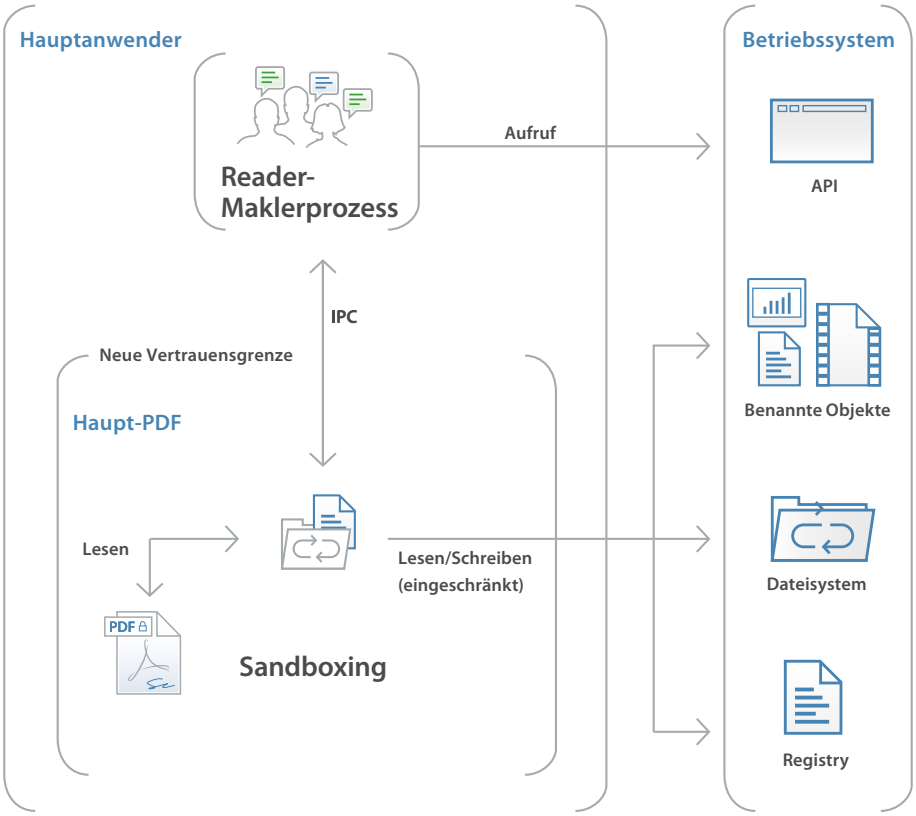
Geschützte Ansicht in Acrobat DC

Ähnlich wie der geschützte Modus von Acrobat Reader DC ist die geschützte Ansicht von Acrobat DC eine Implementierung der Sandbox-Technologie. Bei Acrobat DC werden in dieser Ansicht nicht nur das Schreiben von schadhaftem Code auf Ihrem Computer-System mithilfe einer PDF-Datei unterbunden, sondern auch das Auslesen vertraulicher Daten oder geistigen Eigentums.

Die geschützte Ansicht beschränkt die Ausführung nicht vertrauenswürdiger Programme (z. B. eine PDF-Datei mit von ihr aufgerufenen Prozessen) auf eine isolierte Umgebung – die „Sandbox" –, um zu verhindern, dass schädlicher Code in der Datei den Rechner beeinträchtigt.

Bei der geschützten Ansicht wird davon ausgegangen, dass alle PDF-Dateien potenziell schädlich sind. Daher wird jede Ausführung auf die Sandbox beschränkt, es sei denn, Sie haben eine Datei als vertrauenswürdig gekennzeichnet. Dieser Schutz beim Öffnen von PDF-Dokumenten steht sowohl in Acrobat DC als auch im Browser zur Verfügung. Die geschützte Ansicht wird unter Windows 8 und höher in einem AppContainer ausgeführt. Dadurch entsteht eine noch besser abgeschirmte Umgebung.

Oben im Anzeigefenster wird eine gelbe Meldungsleiste eingeblendet, sobald Sie eine potenziell schädliche Datei in der geschützten Ansicht öffnen. Diese Leiste weist darauf hin, dass eine nicht vertrauenswürdige Datei in der geschützten Ansicht geöffnet wurde, in der viele Acrobat DC-Funktionen deaktiviert und die Möglichkeiten der Interaktion mit der Datei eingeschränkt sind. Die Datei ist schreibgeschützt. Eingebettete oder verknüpfte schädliche Inhalte können in Ihr System nicht eindringen. Um die Datei als vertrauenswürdig zu kennzeichnen und alle Funktionen von Acrobat DC zu aktivieren, klicken Sie auf „Alle Funktionen aktivieren" in der Meldungsleiste. Acrobat schaltet daraufhin die geschützte Ansicht aus und fügt die Datei zur Liste vertrauenswürdiger Quellen bzw. Elemente hinzu. Ab dem nächsten Öffnen dieser Datei gelten nicht mehr die Einschränkungen der geschützten Ansicht.



Ausführung von JavaScript

Whitelist Framework

JavaScript kann selektiv für Workflows aktiviert werden, indem Sie mithilfe der Option „Vertrauenswürdige Sites" Dokumente in Whitelists aufnehmen. Die Vertrauenswürdigkeit wird aufgrund zertifizierter Dokumente, Microsoft Windows-Sicherheitszonen oder durch Hinzufügen bestimmter Dateien, Ordner oder Hosts erteilt.

Acrobat DC bietet erweiterte Steuerungen für JavaScript-basierte Whitelists und Blacklists unter einer Vielzahl von Umgebungen wie Microsoft Windows oder Macintosh. Mit dem Adobe JavaScript Whitelist Framework können Sie selektiv JavaScript für bestimmte PDF-Dateien, Websites, Hosts oder Dokumente aktivieren, die mit einem vertrauenswürdigen Zertifikat signiert sind. Außerdem kann mithilfe des Adobe JavaScript Blacklist Frameworks JavaScript in Geschäftsabläufen verwendet werden, während Anwender und Systeme vor Angriffen geschützt bleiben, die auf bestimmte JavaScript-API-Aufrufe ausgerichtet sind. Wenn ein bestimmter JavaScript-API-Aufruf der „schwarzen Liste" hinzugefügt wird, können Sie ihn sperren, ohne JavaScript vollständig deaktivieren zu müssen. Sie können auch einzelne Anwender daran hindern, die Sperre eines bestimmten JavaScript-API-Aufrufs aufzuheben, sodass der Schutz vor Schad-Software für Ihr gesamtes Unternehmen erhöht wird.

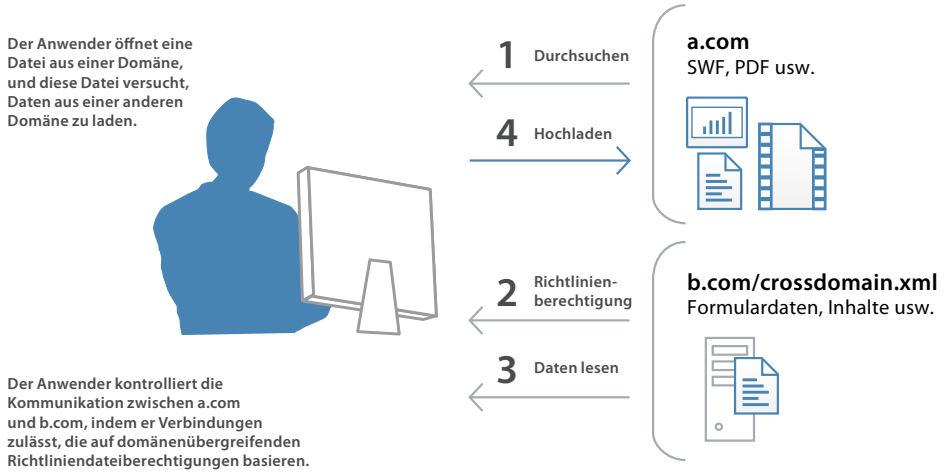
Domänenübergreifende Konfiguration

Standardmäßig wird bei Acrobat DC der uneingeschränkte domänenübergreifende Zugriff für Windows- und Mac OS X-Clients eingeschränkt, damit Angreifer Multimedia-PDF-Dateien nicht dazu nutzen können, auf Ressourcen in einer anderen Domäne zuzugreifen.

Durch die integrierte Unterstützung für Server-basierte domänenübergreifende Richtliniendateien können Sie den domänenübergreifenden Datenzugriff für Acrobat DC und Acrobat Reader DC zulassen. Diese Datei ist ein XML-Dokument. Sie enthält die Richtlinien für domänenübergreifenden Zugriff und befindet sich in der entfernten Domäne. Die Datei gewährt Zugriffsrechte auf die Ausgangsdomäne und gestattet es Acrobat DC oder Acrobat Reader DC, die Transaktion fortzuführen.

In den folgenden Situationen sollten Sie die domänenübergreifende Unterstützung von Adobe aktivieren:

- Wenn domänenübergreifender Zugriff erforderlich ist und sonstige Funktionen genutzt werden sollen, etwa die Erkennung aufgrund eines digitalen Zertifikats
- Wenn domänenübergreifende Zugriffsrechte von nur einem Server-basierten Standort aus verwaltet werden sollen
- Wenn Sie Workflows implementieren, die Datenanforderungen aus mehreren Domänen zur Rückgabe von Formulardaten, SOAP-Anforderungen, Referenzierung von Stream-Medien sowie .NET-HTTP-Anforderungen enthalten



Benutzerfreundliche Sicherheitsmeldungen

Zusätzlich zu Prozessen für die Reaktion auf Zwischenfälle und Sicherheitswarnungen implementiert Acrobat DC eine benutzerfreundliche Methode mit Sicherheitsmeldungen über die gelbe Meldungsleiste. Wenn die erweiterte Sicherheit aktiviert ist und die PDF-Datei nicht als privilegiert oder vertrauenswürdig eingestuft wurde, erscheint die Leiste, wenn die Datei versucht, eine möglicherweise riskante Aktion auszuführen, z. B.:

- Domänenübergreifenden Zugriff aufrufen
- Privilegiertes JavaScript ausführen
- Eine von JavaScript aufgerufene URL aufrufen
- Eine in die „schwarze Liste“ eingetragene JavaScript-API aufrufen
- Daten einfügen
- Skripte einfügen
- Eingebettete Multimedia-Elemente wiedergeben

In Acrobat DC und Acrobat Reader DC erscheint die Leiste im oberen Dokumentbereich mit einer Warnung beziehungsweise Fehlermeldung. Der Anwender kann auswählen, ob er dem Dokument „Einmal“ oder „Immer“ vertrauen möchte. Wenn Sie „Immer“ wählen, wird das Dokument der Liste privilegierter Dokumente hinzugefügt.

Wenn Anwender eine Datei erhalten, können sie die Stufe der Vertrauenswürdigkeit über die Schaltfläche „Optionen“ einrichten. Unternehmensweit können Sie die Vertrauenswürdigkeit für Dateien, Ordner und Hosts vorab konfigurieren, sodass die Meldungsleiste in einem vertrauenswürdigen Unternehmens-Workflow nie angezeigt wird.

Cloud-Sicherheit

Alle Cloud-Dienste, Systeme und Prozesse werden von Adobe kontinuierlich überwacht und laufend optimiert, um den steigenden Ansprüchen und Herausforderungen zum Thema Sicherheit und Datenschutz gerecht zu werden. Die Dienste von Document Cloud, darunter Adobe Sign und die von Acrobat DC genutzten PDF-Dienste, sind darauf ausgelegt, die Vertraulichkeit, Integrität und Verfügbarkeit von Dokumenten sicherzustellen. Document Cloud-Dienste sind mit ISO 27001, PCI DSS und SOC 2 Type 2 konform und erfüllen viele zusätzliche branchenspezifische Zertifizierungen, Standards und Vorgaben. Ausführliche Informationen zu diesem Thema finden Sie im *Überblick über die Sicherheit der Adobe Document Cloud*.

Sicherheit im Rechenzentrum

PDF-Dienste sowie die Datenspeicherung für Document Cloud werden in Rechenzentren der Kategorie „Tier 4" des American National Standards Institute (ANSI) gehostet und von Amazon Web Services (AWS) verwaltet, unserem bevorzugten Anbieter für Cloud-Dienste. Amazon Web Services (AWS) führt äußerst strenge Kontrollen in Bezug auf den Zugriff auf Rechenzentren, Fehlertoleranz, Umgebungssicherung und Sicherheit durch. Nur zugelassene, autorisierte Adobe-Mitarbeiter, Mitarbeiter bei Anbietern von Cloud-Diensten und Vertragspartner mit einem legitimen und akkreditierten Unternehmen haben Zugriff auf den gesicherten Standort in Virginia (USA). Ausführliche Informationen zur Sicherheit der Rechenzentren von Amazon Web Services finden Sie unter *https://aws.amazon.com/de/security/*

Verschlüsselung und Schutz von Daten

Bei der Entwicklung von Adobe-Produkten und -Diensten – einschließlich Document Cloud-Diensten – steht Datenschutz an erster Stelle. Im Ruhemodus werden Dokumente und Dateien mit dem Standard 256-Bit-AES verschlüsselt, der vom amerikanischen National Institute of Standards and Technology (NIST) festgelegt wurde. Um die sichere Datenübertragung zu gewährleisten, wird HTTP (Hypertext Transfer Protocol) in Verbindung mit TLS-Verschlüsselung (Transport Layer Security) unterstützt.

Der Zugriff auf Kundendaten für bestimmte Geschäfts- und Support-Aktivitäten ist auf bestimmte Document Cloud-Mitarbeiter und autorisierte Partner beschränkt. Adobe bietet keiner Behörde direkten oder systematischen Zugriff auf gespeicherte Kundendaten. Weitere Informationen zu Adobes Richtlinien für Datenschutz finden Sie unter *www.adobe.com/de/privacy*.

Integration mit Systemarchitekturen

Permanent aktive Sicherheit

Acrobat DC nutzt mithilfe einer weiteren Verteidigungsebene gegen Angriffe, die versuchen, die Kontrolle über Desktop-Systeme zu übernehmen oder den Arbeitsspeicher zu beschädigen, integrierte, permanent aktivierte Sicherheitsmaßnahmen unter Windows und Mac OS X.

Data Execution Prevention (DEP) schränkt die Platzierung von Daten oder schädlichem Code an Stellen im Speicher ein, die vom Windows-Betriebssystem als geschützt definiert sind. Apple bietet einen ähnlichen Schutz für Mac OS X Lion, mit Stack-DEP und Heap-basiertem DEP. Zudem wird dieser Schutz auf 32- und 64-Bit-Programme ausgedehnt, sodass alle Applikationen Angriffen gegenüber weniger anfällig sind.

Address Space Layout Randomization (ASLR) verbirgt Speicher und Verzeichnisse von Systemkomponenten. So wird es für Angreifer schwieriger, die Komponenten zu finden und zu manipulieren. Windows und Mac OS X Lion verwenden ASLR. Unter Mac OS X Lion wurde ASLR außerdem auf 32- und 64-Bit-Programme erweitert.

Registrierungsebene und Plist-Konfiguration

Acrobat DC bietet Ihnen eine Reihe von Werkzeugen zur Verwaltung der Sicherheitseinstellungen, etwa Voreinstellungen für die Registrierungsebene (Windows) und für die Plist (Mac OS). Mit diesen Voreinstellungen können Sie Clients konfigurieren, sowohl vor als auch nach der Bereitstellung, um Folgendes zu erreichen:

- Erweiterte Sicherheit aktivieren oder deaktivieren
- Vertrauenswürdige Sites aktivieren oder deaktivieren
- Vordefinierte vertrauenswürdige Sites angeben
- Bestimmte Funktionen sperren und die Benutzerschnittstelle der Anwendung deaktivieren, sodass die Endanwender die Voreinstellungen nicht ändern können
- Nahezu sämtliche anderen sicherheitsrelevanten Funktionen deaktivieren, aktivieren oder konfigurieren

Einfache Bereitstellung und Verwaltung

Höhere Software-Sicherheit

Die geschützte Ansicht ist nur ein Beispiel für die umfangreiche Entwicklungsarbeit an Acrobat DC zum Schutz vor Bedrohungen. Durch den höheren Schutz gegen Fremdeinwirkung werden die Anzahl außerplanmäßiger Sicherheits-Updates verringert und die Dringlichkeit geplanter Updates heruntergesetzt. All diese Punkte erhöhen die Flexibilität und senken die Gesamtbetriebskosten, insbesondere in Umgebungen mit hohen Anforderungen an die Sicherheit.

Unterstützung für Citrix und Applikationsvirtualisierung

Nutzen Sie anwendergebundene Lizenzen in virtuellen Umgebungen wie Citrix XenApp, Citrix XenDesktop, VMware Horizon und Microsoft App-V, um Mitarbeitern von überall sicheren Zugriff auf Acrobat-Funktionen zu gewähren.

Unterstützung für Enterprise Mobility Management-Lösungen

Mit Adobe können Unternehmen Lösungen für mobiles Arbeiten implementieren, ohne Abstriche bei Sicherheit und Compliance machen zu müssen. Sowohl die Acrobat Reader-App als auch die Adobe Sign-App unterstützt die EMM-Plattform Android for Work, und Adobe Acrobat Reader für Microsoft Intune ist für Android und iOS verfügbar. Darüber hinaus unterstützt Acrobat Reader die AppConfig-Plattform. Erfahren Sie mehr über die *IT-Ressourcen* von Adobe.

Unterstützung für Windows Server Group Policy Objects und Microsoft Active Directory

Windows Server Group Policy Objects (GPO) und Microsoft Active Directory ermöglichen die Automatisierung einer zentralen Verwaltung zahlreicher Computer-Systeme. Adobe unterstützt jetzt zusätzlich zertifizierte Vorlagen für Microsoft Active Directory Administrative (ADM) für Gruppenrichtlinien in Acrobat DC. Das ermöglicht Software-Installationen bei Bedarf sowie eine automatische Reparatur von Applikationen. Falls eine Applikation nach der Implementierung konfiguriert werden muss, können Sie mit ADM-Vorlagen die erforderlichen Einstellungen unternehmensweit umsetzen.

Unterstützung für Microsoft SCCM und SCUP

Sie können über den Microsoft System Center Configuration Manager (SCCM) Aktualisierungen effizient importieren und veröffentlichen, damit gewährleistet ist, dass die von Ihnen verwalteten Windows-Desktops immer auf dem neuesten Sicherheitsstand sind.

Über Microsoft System Center Publisher-Kataloge (SCUP) lässt sich die Aktualisierung aller Acrobat DC-Installationen innerhalb einer Organisation automatisieren. Außerdem erleichtern sie die Erstimplementierung von Adobe-Software. SCUP kann automatisch Updates von Adobe importieren, sobald sie verfügbar sind, damit die Aktualisierung Ihrer Acrobat DC-Implementierungen vereinfacht wird. Die Integration mit SCCM/SCUP verringert die Gesamtbetriebskosten für Adobe-Produkte, da Patches in der gesamten Organisation einfacher und schneller installiert werden können.

Unterstützung für das Apple Package-Installationsprogramm und für Apple Remote Desktop

Adobe hat das standardmäßige Apple Package-Installationsprogramm aus dem Lieferumfang von Mac OS X anstelle des eigenen Adobe-Installationsprogramms implementiert. Dadurch wird es einfacher, Acrobat auf Macintosh-Desktops im Unternehmen zu installieren, weil Sie mit Apple Remote Desktop die Erstimplementierung und die nachfolgenden Upgrades und Patches zentral verwalten können.

Kumulative, regelmäßige Updates und Patches

Damit Ihre Software immer auf dem neuesten Stand ist, stellt Adobe in regelmäßigen Zeitabständen Updates mit Funktions-Upgrades und Bugfixes bereit. Im Bedarfsfall werden außerplanmäßige Patches veröffentlicht. Adobe setzt möglichst oft kumulative Patches ein, um den Arbeits- und Zeitaufwand für die Systemaktualisierungen zu minimieren. Alle Sicherheits-Patches werden intensiv getestet, bevor sie freigegeben werden, damit die Kompatibilität mit vorhandenen Installationen und Abläufen gewährleistet ist.

Geplante Updates werden jeweils im Blog des Adobe Product Security Incident Response Team unter *blogs.adobe.com/psirt* angekündigt.

Die neuesten Sicherheitsbulletins und -hinweise über Adobe-Produkte finden Sie unter *www.adobe.com/de/support/security*. Detaillierte Hinweise zu Adobe-Produkten und Sicherheitsfunktionen finden Sie in Adobes Bibliothek für Anwendungssicherheit unter *www.adobe.com/go/learn_acr_appsecurity_en*.

Adobe Customization Wizard und Enterprise Toolkit

Für eine bessere Kontrolle über Ihre unternehmensweiten Installationen stellt Adobe die folgenden Werkzeuge zur Verfügung:

- **Adobe Customization Wizard** – Unterstützt IT-Experten kostenlos bei der Anpassung des Acrobat-Installationsprogramms und der Anwendungsfunktionen vor der Bereitstellung.
- **Adobe Enterprise Toolkit (ETK) für Acrobat und Windows** – Eine Applikation, die sich automatisch aktualisiert, sich beliebig anpassen lässt und die Adobe Preference Reference enthält. Das Adobe ETK umfasst außerdem eine ständig gepflegte Liste mit interessanten Ressourcen für Administratoren in Unternehmen und Organisationen.

Mehr über diese Werkzeuge erfahren Sie auf der Seite *IT-Ressourcen*.

Fazit

Bei Acrobat DC hat die Sicherheit von PDF-Dokumenten und die Ihrer Daten oberste Priorität. Acrobat DC ist mit dem Hauptaugenmerk auf dem Aspekt Sicherheit konzipiert. Das betrifft den verbesserten Anwendungsschutz vor dem Diebstahl vertraulicher Daten und geistigen Eigentums genauso wie das Blockieren der Installation von Schad-Software auf Ihren Computer-Systemen. Dazu zählen aber auch Werkzeuge zur einfacheren unternehmensweiten Bereitstellung und Verwaltung. Insgesamt profitieren Sie von erheblich geringeren Gesamtbetriebskosten gegenüber den früheren Acrobat-Versionen.

Weitere Informationen

www.adobe.com/de/security/

Adobe

Adobe Systems GmbH
Georg-Brauchle-Ring 58
D-80992 München
Adobe Systems (Schweiz) GmbH
World Trade Center
Leutschenbachstrasse 95
CH-8050 Zürich
www.adobe.de
www.adobe.at
www.adobe.ch
www.adobe.com

7/17